Threat Analysis in Wireless 802.11 Networks

Giuseppe Razzano[1], Neeli R. Prasad[2], Roberto De Paolis[3], Roberto Cusani[3]

[1] Telecommunication Research Center Vienna (ftw.), Austria
[2] Center for TeleInFrastruktur (CTIF), Aalborg University, Denmark
[3] INFOCOM Dpt., University of Rome "La Sapienza", Italy
email: *razzano@ftw.at; np@kom.aau.dk; robbyrm@tiscali.it; robby@infocom.uniroma1.it*

INTRODUCTION

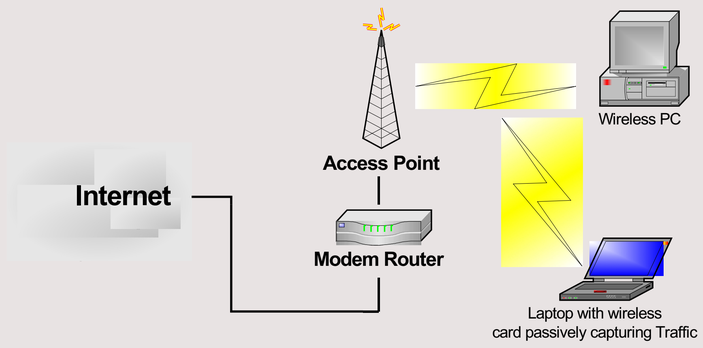
- Due to the diffusion of internet based services, a large number of people require **secure and protect information exchange**, also in their private life.
- Ease of installation, reduced costs, scalability are among the reasons that have led to an **enormous diffusion of wireless systems**. An ever increasing number of private houses and small offices are now equipped with wireless access.
- Federal security agency in USA has announced that unsecured Wi-Fi networks of unsuspecting consumers and businesses have started to be used by criminals.
- While in the wired world, it was often difficult for lawbreakers to make themselves untraceable, in the wireless world, on the contrary, it is extremely easy, especially thanks to the amount of open and unsecure Wi-Fi networks.
- This work presents the result of some tests carried on to analyze the security level of the current installations of 802.11 networks, **analysing the main problems and vulnerabilities** and **proposing some countermeasures to** increase the security level, given the current wireless devices available.

HOW TO SECURE A WLAN

- Choose network cards that support 128-bit encryption or **256-bit encryption**.
- **Intrusion Detection Systems** (IDS) must be in place to monitor each segment of the wireless network, in order to recognize and prevent attacks, before the hacker authenticates to the AP. Generally speaking, IDS comprises of three functional areas:
  - A stream source that provides chronological event information.
  - An analysis mechanism to determine potential or actual intrusions.
  - A response mechanism that takes action on the output of the analysis.
- When the expense of IDS technology cannot be sustained, some **techniques** can be applied to **discover wireless card** trying to hack the WLAN or sniffing its traffic:
  - Wireless cards running in promiscuous mode can be detected sending a request to the IP address of the machine, but not to its WLAN adapter.
  - *Decoy method*: setting up a client and a *fake* server on either side of the network, where the client runs a script to logon to the server using protocol where user authentication is sent in plain text (e.g. Telnet, POP, IMAP) . Once a hacker sifts the usernames/passwords, he/she will then attempt to log on using this information, *on the server which* log this occurrence, alerting the fact that a sniffing hacker has found the traffic and attempted to use the information.
- **Disable beacons** on the AP, such that only nodes knowing the SSID can associate to the AP. However, this action does not prevent WLAN identification, as some scanners operate by sending a steady stream of broadcast packets on all possible channels and unfortunately, APs respond to broadcast packets, reporting their existence, even if beacons have been disabled.
- Use **MAC** level **filtering.** MAC addresses can be spoofed, but still MAC filtering is enough to thwart off casual hackers. This solution is not scalable, but it is a good choice for SOHO scenarios, where the number of users is not large and does not change very often.
- Do **not use DHCP** on WLANs. To access hosts at a targeted site, a hacker would need to obtain a valid IP configuration. Static IP address require the user to correctly configure its pc to access the network, but in all the cases where the number of users does not change often this solution is suitable.
- **Locate APs centrally**, thus placing them away from the exterior walls or windows and adjust their transmission power (50-75% reduction can be achieved.
- **Change encryption keys**. An attacker could crack the keys within a matter of hours, but changing the encryption keys ensures that a compromised network does not remain insecure indefinitely.
- **Change default passwords/IP addresses**. Most APs have a built in web server that provides a console for administration.
- Purchase only APs that have **flashable firmware**. There are security enhancements that are being developed and released very frequently.
- **Virtual Private Networks** (VPNs) should be used to increase what 802.11b provides in the way of encryption and authentication.

WAR DRIVING

War driving means **going around in an inhabited area**, while **scanning for wireless access points**.



Hacking a WLAN, the first problem is to **locate and detect the wireless network**.

Beacons sent by APs at predefined intervals are essentially invitations and driving directions that enable the client to easily find the AP and configure the appropriate settings to communicate.

WLAN scanners allow users to identify WLANs through the use of a wireless **Network Interface Card** (NIC), **running in promiscuous mode**, and the **application of a software tool, able to probe for APs** (e.g. *NetStumbler*)**.** Another useful tool is a Network Sniffer. This, can be used, either as SSID and MAC address identifier, or as a wireless sniffer to cache all the traffic of the WLAN in order to decrypt it.

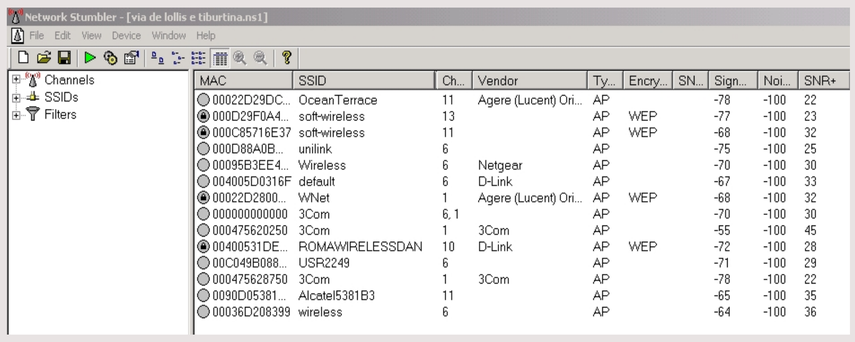
To test the level of security and the diffusion of wireless network devices, several war driving in the city of Rome were carried on.

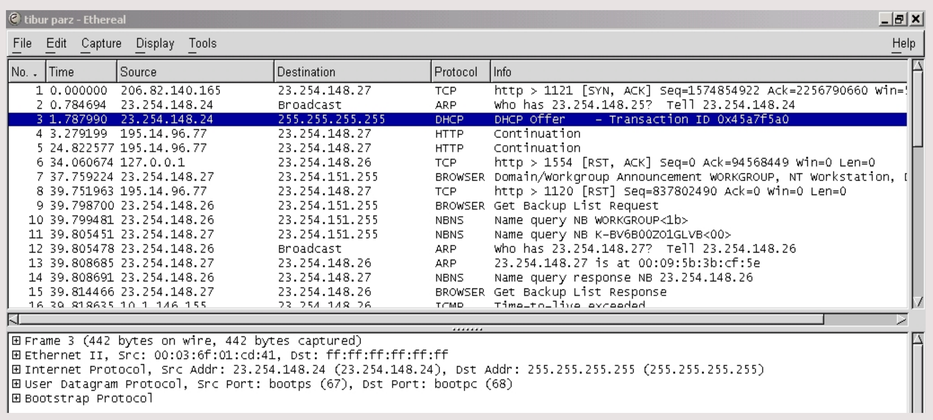
.

War Driving Configuration
Notebook Prostar 2794
512 Mega Ram
Windows 2000 Professional S.P. 4
WLAN Card Asus WL-100g
NetStumbler 0.3.30
Ethereal 0.9.14 (with WinpCap 3.01)

During the scanning, a large number of APs, installed in hotels, flats and small offices were located: the **level of security** of the AP was **very low**, and it was possible, almost always, to **easily surf on the discovered networks**.

Cracking time is dependent upon both the key size and the amount of traffic in the network. When network traffic is near the capacity of 11 MBps, cracking a 40-bit WEP key may take from three to four hours. To facilitate the WEP cracking, it is possible to artificially generate network traffic using an UDP flooder.


Network Stumbler - [via de lollis e tiburtina.ns1]
File Edit View Device Window Help
Channels
SSIDs
Filters
MAC SSID Ch... Vendor Ty... Encry... SN... Sign... Noi... SNR+
00022D29DC... OceanTerrace 11 Agere (Lucent) Ori... AP -78 -100 22
000D29F0A4... soft-wireless 13 AP WEP -77 -100 23
000C85716E37 soft-wireless 11 AP WEP -68 -100 32
000D88A0B... unilink 6 AP -75 -100 25
00095B3EE4... Wireless 6 Netgear AP -70 -100 30
004005D0316F default 6 D-Link AP -67 -100 33
00022D2800... WNet 1 Agere (Lucent) Ori... AP WEP -68 -100 32
000000000000 3Com 6, 1 AP -70 -100 30
000475620250 3Com 1 3Com AP -55 -100 45
00400531DE... ROMAWIRELESSDAN 10 D-Link AP WEP -72 -100 28
00C049B088... USR2249 6 AP -71 -100 29
000475628750 3Com 1 3Com AP -78 -100 22
0090D05381... Alcatel5381B3 11 AP -65 -100 35
00036D208399 wireless 6 AP -64 -100 36



IEEE 802.11 SECURITY ENHANCEMENT

802.11i is the new version of the standard, finalized in 2004 by IEEE Taskgroup i, with the aim of solving the weaknesses of WEP-based wireless security. Substantial components of the 802.11i standard were already released before the standard was released and products are available on the market, under the auspices of the **Wi-Fi** Alliance. Already in November 2002, the Wi- Fi Alliance announced the so called **Wireless Protected Access** (**WPA**)**.**

- **802.1X port-based authentication framework**: extensible authentication protocol that applies to both wireless and wired Ethernet networks.These are the main advantages:
  - Standard based: 802.1x is an IEEE standard released in June 2001, which makes use of existing standards (i.e. Extensible Authentication Protocol (EAP) and RADIUS).
  - Flexible authentication: administrators may choose the type of authentication method used.
  - Scalable to large enterprise networks by simply adding APs and, as needed, additional RADIUS servers.
  - Centrally managed allowing roaming to be made as transparent as possible.
- **Client key**s are **dynamically generated** and **propagated**. The encapsulation protocol (EAP) allows different authentication protocols to be used (i.e. Md5, LEAP, EAP-Transport Layer Security (TLS) - Public Key Infrastructure (PKI), EAP-Tunneled TLS (TTLS)).
- **Temporal Key Integrity Protoco**l (TKIP): enables secure, dynamic key generation and exchange. TKIP continues to use the RC4 encryption engine used by WEP, but provides the following important improvements over WEP:
  - Dynamic keys: allows per-session and per-packet dynamic ciphering keys.
  - Message integrity checking (MIC): ensures that message have not been tampered during transmission.
  - 48-bit IV hashing provides longer IV (used in conjunction with a base key to encrypt and decrypt data) that avoids the weaknesses of the shorter 24-bit WEP RC4 key.